

Quantum-enhanced tomography of unitary processes

Xiao-Qi Zhou^{*,†,1}, Hugo Cable^{*,‡,2,1}, Rebecca Whittaker^{*,1}, Peter Shadbolt¹, Jeremy L. O'Brien¹, Jonathan C. F. Matthews^{§,1}

¹ Centre for Quantum Photonics, H. H. Wills Physics Laboratory and Department of Electrical and Electronic Engineering, University of Bristol, Merchant Venturers Building, Woodland Road, Bristol BS8 1UB, UK.

² Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543

A fundamental task in photonics is to characterise an unknown optical process, defined by properties such as birefringence, spectral response, thickness and flatness. Amongst many ways to achieve this, single-photon probes can be used in a method called quantum process tomography (QPT). Furthermore, QPT is an essential method in determining how a process acts on quantum mechanical states. For example for quantum technology, QPT is used to characterise multi-qubit processors¹ and quantum communication channels²; across quantum physics QPT of some form is often the first experimental investigation of a new physical process, as shown in the recent research into coherent transport in biological mechanisms³. However, the precision of QPT is limited by the fact that measurements with single-particle probes are subject to unavoidable shot noise—this holds for both single photon and laser probes. In situations where measurement resources are limited, for example, where the process is rapidly changing or the time bandwidth is constrained, it becomes essential to overcome this precision limit. Here we devise and demonstrate a scheme for tomography which exploits non-classical input states and quantum interferences; unlike previous QPT methods our scheme capitalises upon the possibility to use simultaneously multiple photons per mode. The efficiency—quantified by precision per photon used—scales with larger photon-number input states. Our demonstration uses four-photon states and our results show a substantial reduction of statistical fluctuations compared to traditional QPT methods—in the ideal case one four-photon probe state yields the same amount of statistical information as twelve single probe photons.

Quantum information protocols promise new capabilities for a range of computational, communication and sensing applications. Successful development and implementation of all these quantum information protocols rely on efficient techniques to characterise quantum devices. The most widely-used method for this purpose is QPT—in which a mathematical description of a quantum process is reconstructed by estimating the probabilities of outcomes for a selection of probe states and measurement settings. QPT has been demonstrated in a variety of physical systems, including ion traps⁵, nuclear magnetic resonance⁶, superconducting circuits⁷ and Nitrogen-vacancy colour centres⁸. In the context

of photonics, experimental demonstrations have been reported in e.g. Refs.^{1,9–11} for linear-optical systems using few-photon states. (A continuous-variable version of QPT has also been demonstrated for general optical quantum processes using coherent-state inputs and homodyne measurements¹².)

Despite the success of QPT on small systems, there remains scope for improvement. For example, a well-known problem for QPT is the requirement for an exponentially-growing number of measurements for processes on an increasing number of qubits. Many methods have been devised and demonstrated to circumvent this problem, such as efficient state tomography¹³ and compressed sensing¹⁴. In photonics, photon loss and interferometric instability present the main challenges, and a method called “super-stable tomography” was recently proposed to address these¹⁵. Here we are concerned with improving measurement precision given a fixed number of particles propagating through the unknown process. It has been found that the precision achieved by tomography methods after a fixed number of measurements are dependent on the unknown state or process. This has naturally led to adaptive schemes^{16,17} where dynamic measurement settings are used. Fundamentally, whatever measurement scheme is used—adaptive or non-adaptive—the precision is always limited by the unavoidable statistical fluctuation, where the ultimate precision limits are dictated by quantum mechanics.

Our approach is to exploit quantum interferences to minimize the unwanted fluctuation on the quantum-process measurement statistics by drawing upon techniques from quantum metrology⁴. Here we present a quantum-enhanced process tomography protocol which works for arbitrary unitary optical processes on two modes, and experimentally demonstrate measurement precision beyond that achievable with traditional QPT protocols. We first explain the theory of our protocol, and then present the results of our experimental implementation which show evidence for a quantum-enhanced precision compared to the conventional QPT approach. Finally, we discuss generalisations and applications of our protocols.

The standard procedure for QPT applies repeated state tomography on a set of input states acted on by the process^{1,18}. A full procedure for process tomography commonly assumes that the quantum process corresponds mathematically to completely-positive trace-preserving map and physically to quantum evolution which can include decoherence or dissipation. If the process acts on a l -dimension system, $l^4 - l^2$ configurations must be tested¹⁸. Here we consider the unitary case where there are $l^2 - 1$ unknown real parameters, encompassing a broad class of optical devices and processes. For the case of two-mode unitaries ($l = 2$), there are 3 real

*These authors contributed equally

[†]Email: Xiaoqi.Zhou@bristol.ac.uk

[‡]Email: Hugo.Cable@bristol.ac.uk

[§]Email: Jonathan.Matthews@bristol.ac.uk

parameters that need to be determined and they correspond to the complex transmission amplitude $a + ib$ and the complex reflection amplitude $c + id$. So the task to estimate the unknown unitary U becomes to determine the values of a , b , c and d satisfying the unitarity constraint

$$a^2 + b^2 + c^2 + d^2 = 1. \quad (1)$$

We assume that the unitary is operating on the polarisation degree of freedom and we denote horizontal (diagonal, right circular) and vertical (anti-diagonal, left circular) polarisation by H (D, R) and V (A, L), where $|D/A\rangle = \frac{1}{\sqrt{2}}(|H\rangle \pm |V\rangle)$ and $|R/L\rangle = \frac{1}{\sqrt{2}}(|H\rangle \pm i|V\rangle)$. By inputting an H (D, R) photon to the unitary and measuring the output photon in the H/V (D/A, R/L) basis, the probability of detecting H (D, R) polarisation at the output is p_{HV} (p_{DA} , p_{RL}), where

$$\begin{aligned} p_{HV} &= a^2 + b^2, \\ p_{DA} &= a^2 + d^2, \\ p_{RL} &= a^2 + c^2. \end{aligned} \quad (2)$$

By using the unitary constraint of Eq. 1, U can then be estimated by measuring these three probabilities. There is a discrete set of estimates, which all correspond to the same values for $p_{HV(DA,RL)}$. (A similar situation exists in interferometric phase estimation where typically multiple values of the phase are consistent with a particular set of data.) While the sign of a can always be fixed to positive, the signs of b , c and d need to be resolved. For this we use supplementary standard QPT, using a small and minimal number of probe photons, to provide an initial coarse-grained estimate sufficient to differentiate these alternatives (See Methods).

The traditional approach would directly estimate p_{HV} , p_{DA} and p_{RL} with single photons by looking at the ratio of detections at the two outputs. The precision of estimating p_{HV} is $\Delta p_{HV} = \sqrt{p_{HV}(1-p_{HV})/N}$ which scales as $O(N^{-1/2})$, the standard quantum limit (SQL) for measurement. To go beyond the SQL, our approach uses multi-photon states as probes, determining the three probabilities shown in Eq. 2, indirectly from the multi-photon counting statistics.

The multi-photon input state we use is a N -photon state split equally between H- and V-polarisation¹⁹, $|N/2, N/2\rangle_{HV}$, where N is even. After propagating through the unknown unitary, the state is measured in the H/V basis as in the single-photon case. The probability of detecting n_H H-polarised photons and n_V V-polarised photons at the output is a function of p_{HV} alone. Explicitly, these probabilities are

$$\mathcal{P}(n_H, n_V, p_{HV}) = \frac{n_V!}{n_H!} \left(\mathcal{L}_{(n_H+n_V)/2}^{(n_H-n_V)/2}(2p_{HV}-1) \right)^2, \quad (3)$$

where $\mathcal{L}_{(n_H+n_V)/2}^{(n_H-n_V)/2}$ denotes the standard associated Legendre polynomial²⁰ with degree $(n_H + n_V)/2$ and order $(n_H - n_V)/2$ (See Supplementary Information). Consequently, p_{HV} can be estimated from the photon-counting data using a maximum-likelihood technique with a precision of $\Delta p_{HV} = \sqrt{p_{HV}(1-p_{HV})/(N(N/2+1))}$, which scales with $O(N^{-1})$ —a quadratic improvement compared to the SQL. For the

(n_H, n_V)	outcome(s) probability
$(0, 4), (4, 0)$	$6p_{HV}^2(1-p_{HV})^2$
$(1, 3), (3, 1)$	$6p_{HV}(1-p_{HV})(2p_{HV}-1)^2$
$(2, 2)$	$(6p_{HV}^2-6p_{HV}+1)^2$

TABLE I: The outcome probabilities of four-photon events for the H/V measurement. Analogous expressions hold for the D/A and R/L measurements.

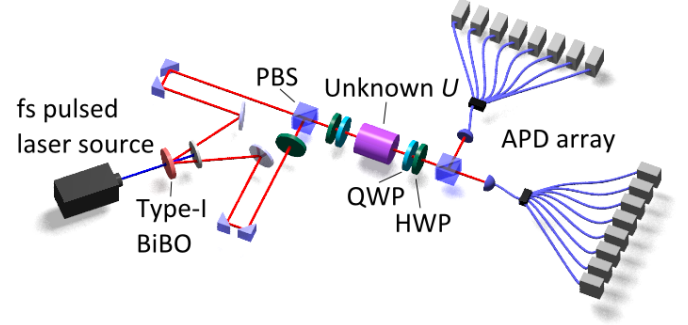


FIG. 1: **Experimental setup for probing the unknown unitary processes.** An 80MHz pulsed Ti-Sapphire laser centred at 808nm is up-converted to 404nm and then focused onto a BiBO (Bismuth Borate) crystal, phase-matched for type-I SPDC, creating non-collinear degenerate horizontally-polarised photon pairs at 808nm. After converting one arm to vertical polarisation using a half-waveplate (HWP, green), the two arms are combined by a polarising beamsplitter (PBS). The resulting state is passed through the unknown unitary (purple) and then measured in the H/V basis. Approximate photon-number counting is implemented on each polarisation mode using a 1-8 fan-out array onto avalanche photodiode detectors (APD, grey). By using different waveplate settings before and after the unknown unitary, the basis for the probe state and measurement can be changed to D/A and R/L.

$N = 4$ case, the outcome probabilities are given in Table I, and the precision of the estimated probability improves by approximately 70%. By changing the input state to $|N/2, N/2\rangle_{DA(RL)}$ and the measurement basis to D/A (R/L), we can obtain p_{DA} (p_{RL}) with the same precision as p_{HV} . It should be noted that it is still not known what kind of quantum advantages can be achieved for the non-unitary processes. Some theoretical results on estimating both unitary and non-unitary processes can be found in References^{21–23}.

To demonstrate our scheme, we use four-photon states generated using standard type-I spontaneous parametric down-conversion (SPDC) (see Fig. 1). With a certain probability, the SPDC source will produce two photon pairs (with H polarisation) across the two arms. After rotating one arm to V polarisation using a half-waveplate (HWP), the two arms are then combined on a polarisation beamsplitter (PBS) thus producing the desired four-photon state $|2, 2\rangle_{HV}$. The state passes through the unknown unitary and is then separated into the H and V components using a PBS. The photon number at each output is resolved using a fan-out array which couples to eight avalanche photodiodes (APDs) (See Methods). We use the measured rates of four-photon outcomes to estimate p_{HV} by using the maximum-likelihood method based on

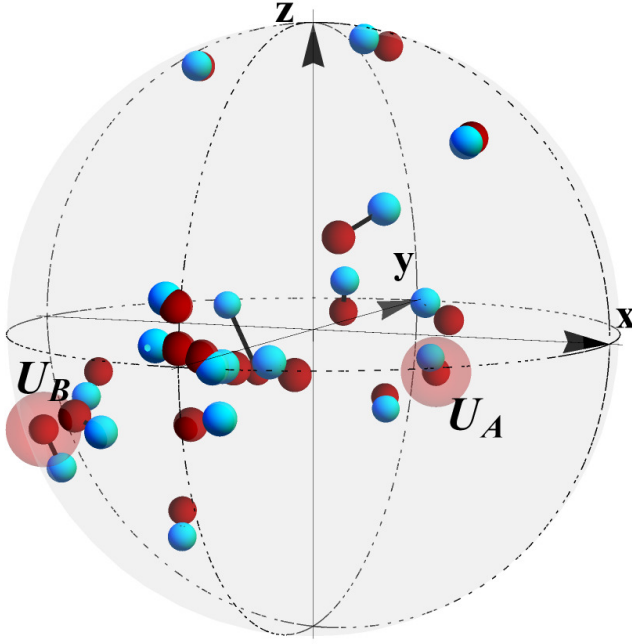


FIG. 2: **Visual representation of 19 randomly-selected unitaries (red) with their experimental reconstructions from four-photon probe states (cyan).** Each of these unitaries was experimentally realised with three consecutive waveplates (HWP, QWP, HWP). The four-photon state $|2, 2\rangle_{HV(DA,RL)}$ is used to probe each unitary and subsequently measured in the H/V (D/A, R/L) basis. The unitaries are then reconstructed from the resulting photon statistics. The representation of each unitary is a point in this unit sphere with coordinates (x, y, z) corresponding to $(-d, c, -b)$. The precision of two highlighted unitaries, U_A and U_B , is subject to detailed analysis with a large data set in Fig. 3.

the theoretical probability distributions shown in Table I. By changing the input state and the measurement basis to D/A (R/L), implemented by waveplates before and after the unitary, we estimate p_{DA} (p_{RL}) in a similar manner. The experimentally determined \tilde{p}_{HV} , \tilde{p}_{DA} and \tilde{p}_{RL} are then used to construct an estimate of the unknown unitary, \tilde{U} . To quantify the discrepancy between \tilde{U} and U we use the process infidelity, defined as $\left(1 - \min_{|\psi\rangle} |\langle\psi|\tilde{U}^\dagger U|\psi\rangle|^2\right)$, where the minimum is taken over all single-photon states $|\psi\rangle$.

To provide evidence that the scheme works for any two-mode unitary, we test it using a number of preselected unitaries randomly sampled from the Haar distribution²⁴. For each of these unitaries U , 200 four-photon probes (800 photons in total) are used to construct the estimate \tilde{U} . The process infidelities range from 96.8% to 99.8%, with a mean of 98.8% showing near-ideal performance for the scheme. The relationships between the expected and the experimentally-reconstructed unitaries are represented graphically in Fig. 2. This analysis shows qualitatively that our scheme provides high-quality estimates for arbitrary unitaries.

Now we turn to the central feature of the scheme—the ability to exploit multi-photon quantum interference to improve

the estimate precision with a fixed input resource—the total number of photons propagating through the unknown unitary. We choose two of these unitaries, $U_A = \begin{pmatrix} 0.70+0.21i & -0.65-0.20i \\ 0.65-0.20i & 0.70-0.21i \end{pmatrix}$ and $U_B = \begin{pmatrix} 0.29+0.34i & 0.33+0.83i \\ -0.33+0.83i & 0.29-0.34i \end{pmatrix}$ (shown in fig. 2), and look at the variation of \tilde{U} over many repetitions of the experiment. Theoretically, both the mean and standard deviation of the process infidelities of \tilde{U} with respect to U will be improved towards zero using our scheme as opposed to the traditional approach using single photons. In practice, we use a SPDC source and post-selection to simulate exact photon-number states, which inevitably result in systematic errors that prevent a fair comparison between the mean infidelities of four-photon and single-photon probe states²⁵. To properly quantify the spread of the estimates \tilde{U} from actual data, we use the standard deviation of the process infidelities of \tilde{U} with respect to U' , where U' is a “central” estimate derived by combining all datasets. The analysis of the experimental data for U_A and U_B are shown in Fig. 3. As expected, the mean and the standard deviation of the infidelity decrease as the photon number increases for both schemes. More importantly, for every fixed input resource, the standard deviation of the infidelity is reduced for our scheme compared to the traditional approach. For example, as shown in Fig. 3, using standard QPT one would need approximately 3600 photons overall to obtain the same small infidelity and spread, as achieved by our protocol using only 1800 probe photons. The experimental results are closely matched to the predictions of the theoretical simulations as described in Fig. 3. In the ideal case, where there is no restriction on the number of probe photons, one four-photon probe state yields the same amount of statistical information as twelve single probe photons. However, our results show a slightly smaller quantum advantage because of practical limitations on the size of the dataset.

The deviations of our experimental results from the theoretical predictions originate from three parts of the experiment—(i) *Input states*: Our scheme assumes perfect Fock states which have fixed photon number. To simulate the Fock states experimentally, we used a SPDC source which inherently contains higher-order terms, temporal distinguishability between photon pairs and spectral distinguishability between the two arms, all of which alter the intended quantum interference; (ii) *Optical components*: There always is imprecision in setting the angles of the manual waveplates, which can be improved by using a motorised bulk-optical system or migrating to an integrated architecture; (iii) *Detection system*: To simulate photon-number resolving detection, we use a 1-to-8 fibre array terminated with 8 APDs on each output. The non-uniform efficiency across the 16 APDs and the non-identical splitting ratio of the fibre arrays result in some bias in the detection system. Despite these limitations, we still see a clear quantum advantage of our four-photon data over the traditional method.

The ability to characterise a quantum process accurately is a basic requirement for demonstrating quantum information techniques, and the method of QPT has been widely deployed. However, it is not well explored how and to what extent it is possible to exceed the precision limit achievable by

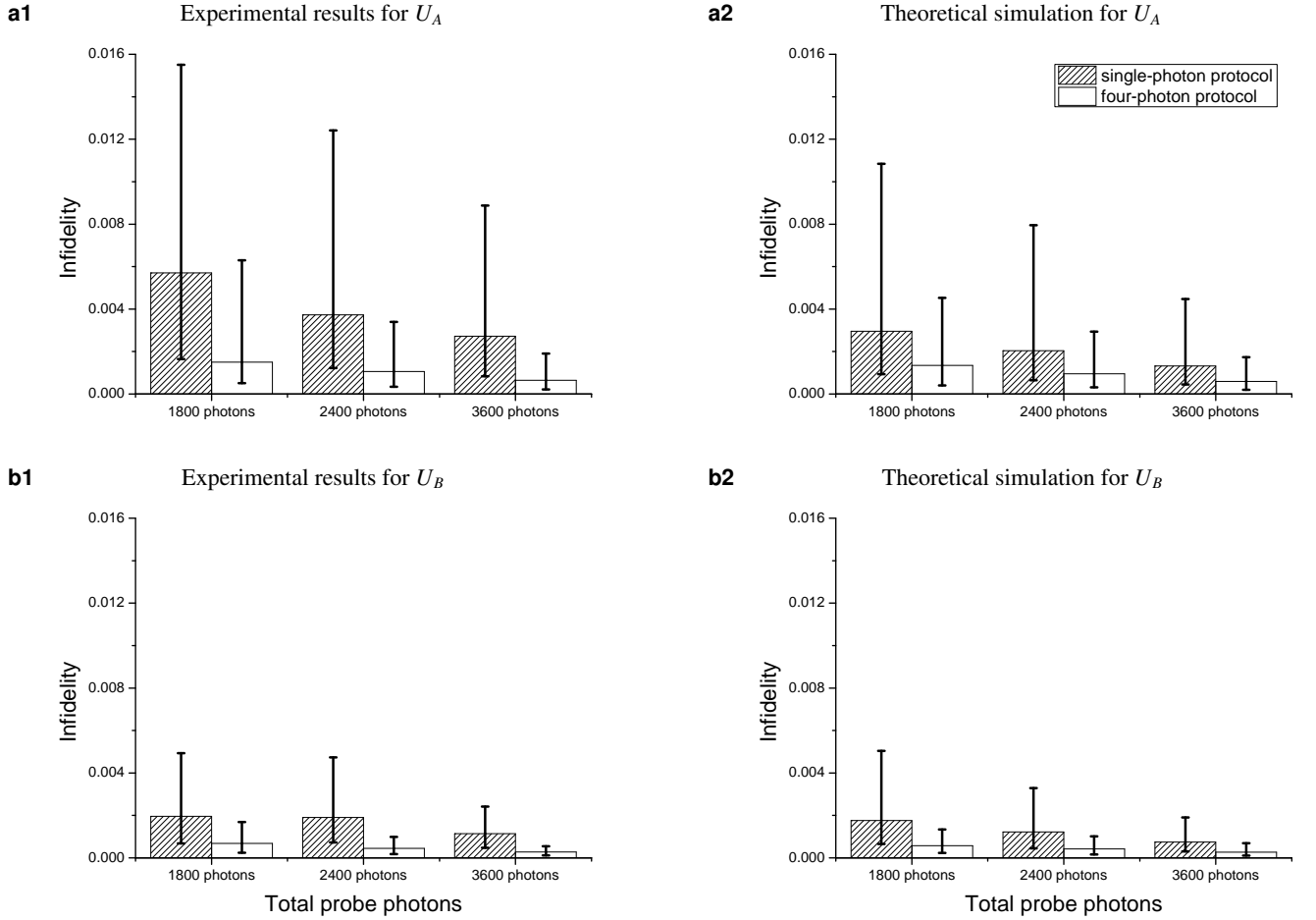


FIG. 3: **Experimental performance of the quantum enhanced tomography protocol using four-photon states.** In this figure, the standard QPT protocol (diagonal fill) using single photons and our method using four photons (unpatterned) are compared, for two unitaries U_A and U_B . To make a fair comparison between the two protocols, the same total number of probe photons are assumed (1800, 2400 and 3600 for all measurements together). **a1** and **b1** are derived from experimental data for U_A and U_B respectively and **a2** and **b2** are based on corresponding theoretical simulations. For each case, the mean infidelity is illustrated, for a series of experimentally-derived estimates \tilde{U}_A or \tilde{U}_B , where the infidelity is defined relative to “central” estimates U'_A or U'_B derived from the accumulated experimental data. Asymmetric lower- and upper-half error bars are used, reflecting the distribution of infidelity values. The data shows that the four-photon version of the protocol achieves greater accuracy and precision than standard QPT with single photons.

QPT. From an alternative perspective, process tomography or unitary estimation, can be regarded as a multi-parameter estimation problem. A general linear-optical unitary on N spatial modes can always be decomposed into multiple variable phases and 50:50 beamsplitters²⁶. Recently, some special families of unitaries using commuting phaseshift operations, with applications in phase imaging²⁷ and interferometry in waveguides²⁸, have been theoretically investigated.

Our protocol, for the general case of a two-mode unitary, corresponds to estimating three unknown non-commuting phases. Since quantum enhancement is well known for single phase estimation in the field of quantum metrology, it is natural to look for an analogous improvement for this multi-parameter problem. We have drawn upon and adapted the techniques from optical phase estimation and successfully achieved a quantum enhancement in estimating a unitary

process. A key strength of this approach is our parametrisation which greatly simplifies the maximum-likelihood procedure. As an aside, we note that there have been several related theoretical investigations which explore how the properties of quantum mechanics, especially quantum entanglement, can improve the precision for abstract unitary estimation^{29–32}. However, these papers adopt different methodologies from our work, and offer no explicit mapping onto photonic systems.

Although our scheme is based on an equal number Fock state in two modes $|N/2, N/2\rangle$ for the input, our method can be conveniently extended with only minor modifications for: (1) Unbalanced input states of the form $|M, N - M\rangle$, and superpositions of these states with different total photon number; (2) Photon-counting techniques with limited ability to discriminate exact photon number³³. The modifications involve changes to the probability distributions used in the

maximum-likelihood estimation procedure, but do not alter the special feature that they always depend on a single parameter (p_{HV} , p_{DA} or p_{RL}). As a practical application, the probe state can be the entire state generated by type-I or type-II parametric downconversion, which can be easily created in the laboratory and is tolerant to photon loss^{25,34}; (3) Unknown unitaries on n modes: the $n^2 - 1$ parameters of such unitaries can be determined by using the same number of input and measurement bases, where for each choice of basis a non-classical multi-photon input state is used. (4) Incorporating an adaptive method. As with standard QPT, the attainable precision of our protocol is dependent on the unknown unitary. As such, by including an adaptive step—updating the measurement bases—the precision can be further improved.

Our protocol can be directly used for optical communication networks³⁵, transferring classical or quantum information, with the purpose of fast and precise characterisation of each link, especially when interferometric stability is required. Our technique also offers a range of applications to the characterisation of optical media and quantum logic gates³⁶, as well as to new types of quantum sensors⁴. Considering applications outside of photonics, the scheme has a natural geometric interpretation bestowed by the Schwinger representation³⁷, which provides a one-to-one map from two-mode- N -photon states to the $N/2$ -spin state space. Here the two-mode unitary operations correspond to physical rotations of a spin system, or equivalently rotations of the reference frame. Consequently, our experiment shows that a quantum advantage is indeed possible for the task of aligning Cartesian reference frames, as predicted in several theoretical works using other protocols³⁸. A spin implementation of our protocol has practical applications for both gyroscopy and magnetometry.

Methods

Reconstruction of U from estimated quantities \tilde{p}_{HV} , \tilde{p}_{RL} , and \tilde{p}_{DA}
Linear inversion of Eq.s 1 and 2 allows the unknown unitary to be reconstructed from the experimental-derived estimates \tilde{p}_{HV} , \tilde{p}_{RL} and \tilde{p}_{DA} , whenever this leads to nonnegative values for \tilde{a}^2 , \tilde{b}^2 , \tilde{c}^2 , or \tilde{d}^2 . This inversion is given explicitly by,

$$\begin{pmatrix} \tilde{a}^2 \\ \tilde{b}^2 \\ \tilde{c}^2 \\ \tilde{d}^2 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ \tilde{p}_{DA} \\ \tilde{p}_{RL} \\ \tilde{p}_{HV} \end{pmatrix}, \quad (4)$$

and it can be applied whenever the following inequalities are all satisfied:

$$\begin{aligned} \tilde{p}_{DA} + \tilde{p}_{RL} + \tilde{p}_{HV} &\geq 1 \\ \tilde{p}_{DA} + \tilde{p}_{RL} - \tilde{p}_{HV} &\leq 1 \\ \tilde{p}_{DA} - \tilde{p}_{RL} + \tilde{p}_{HV} &\leq 1 \\ -\tilde{p}_{DA} + \tilde{p}_{RL} + \tilde{p}_{HV} &\leq 1. \end{aligned}$$

Possible values for the probability estimates define the cube with $0 \leq \tilde{p}_{HV}, \tilde{p}_{RL}, \tilde{p}_{DA} \leq 1$, and the inequalities above determine a tetrahedral subregion which we call the *physical region*—with vertices at (1,0,0), (0,1,0), (0,0,1) and (1,1,1). Outside of the physical region, exactly one of the inequalities fails to hold, and therefore

we choose the point closest to $(\tilde{p}_{HV}, \tilde{p}_{RL}, \tilde{p}_{DA})$ in the physical region (with respect to the Euclidean metric). Simple expressions for the closest point follow from geometric considerations. As an aside, the maximum-likelihood procedure which is applied to estimate the value of $\tilde{p}_{HV(DA,RL)}$ from data, with four-photon input states, cannot distinguish values $\tilde{p}_{HV(DA,RL)}$ and $1 - \tilde{p}_{HV(DA,RL)}$, which are both consistent with measurement results. This is because the probability distributions in Table I and Eq. 3 are symmetric under the mathematical operation $p_{HV} \leftrightarrow 1 - p_{HV}$ (and similarly for $p_{DA/RL}$). This ambiguity is resolved by the same coarse-grained estimates, obtained with supplementary QPT measurements, which is needed to determine the signs of b , c and d .

Supplementary Information

I. PARAMETER DEPENDENCE OF THE PROBABILITY DISTRIBUTIONS FOR MEASUREMENTS IN A FIXED BASIS

Here we identify what information is obtainable from each measurement in our protocol, for an arbitrary (unitary) linear-optical process U on two modes. The action of U on the mode operators is given by,

$$\begin{pmatrix} a_H^\dagger \\ a_V^\dagger \end{pmatrix} = \begin{pmatrix} U a_H^\dagger U^\dagger \\ U a_V^\dagger U^\dagger \end{pmatrix} = \mathcal{M} \begin{pmatrix} a_H^\dagger \\ a_V^\dagger \end{pmatrix} \quad (5)$$

where \mathcal{M} is a unitary two-by-two matrix. The global phase of U is unmeasurable in our setup and hence we assume $\mathcal{M} \in SU(2)$.

\mathcal{M} also corresponds to the linear transformation by U of an arbitrary single-photon superposition state in the Fock basis, $|\psi_1\rangle = c_H|1,0\rangle_{HV} + c_V|0,1\rangle_{HV}$, so that $|\psi_1\rangle \mapsto U|\psi_1\rangle$ is given by $\begin{pmatrix} c_H \\ c_V \end{pmatrix} \mapsto \mathcal{M} \begin{pmatrix} c_H \\ c_V \end{pmatrix}$. We can represent $|\psi_1\rangle$ geometrically on the Bloch sphere with $|0\rangle \equiv |H\rangle$ and $|1\rangle \equiv |V\rangle$ in the usual qubit notation. U then acts by rotating the Bloch vector of $|\psi_1\rangle$ by an angle ϕ around the rotation axis with unit vector \mathbf{n} , where $\mathcal{M} = \exp[-i(\phi/2)\mathbf{n} \cdot \boldsymbol{\sigma}]$ ($\boldsymbol{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$ denotes the Pauli matrices). For an arbitrary N -photon state, $|\psi_N\rangle = \sum_{M=0}^N c_M a_H^\dagger M a_V^\dagger N-M |\text{vac}\rangle$, $U|\psi_N\rangle = \sum_{M=0}^N c_M (a_H^\dagger)^M (a_V^\dagger)^{N-M} |\text{vac}\rangle$, and again the transformation is determined entirely by the coefficients of \mathcal{M} .

Next we look at the general form of the probability distributions for measuring $n_{H(V)}$ horizontally (vertically)-polarized photons at the output, given state $|M, N-M\rangle_{HV}$ at the input, with notation $\mathcal{P}_{HV}(n_H, n_V) = |\langle n_H, n_V |_{HV} U | M, N-M \rangle_{HV}|^2$. ($M = N/2$ in the main text.) We can use an Euler-angle decomposition to write \mathcal{M} as a sequence of rotations on the Bloch sphere about the y and z axes: $\mathcal{M} = \exp[-i(\psi/2)\sigma_z] \exp[-i(\theta/2)\sigma_y] \exp[-i(\xi/2)\sigma_z]$. The z -axis rotations generate phases which do not affect the value of $\mathcal{P}_{HV}(n_H, n_V)$, which therefore depends only on the y -axis rotation with angle θ . As in the main text, we can use p_{HV} to parameterize $\mathcal{P}_{HV}(n_H, n_V)$, and $p_{HV} = \cos^2(\theta/2)$. The probability distributions are given explicitly by rotational Wigner d -matrices as follows,

$$\mathcal{P}_{HV}(n_H, n_V, p_{HV}) = \left[d_{\frac{n_H}{2} - \frac{n_V}{2}, M - \frac{N}{2}}^{\frac{N}{2}} (2 \arccos \sqrt{p_{HV}}) \right]^2. \quad (6)$$

(see Ref.³⁷ for a derivation of the d -matrices). For the case $M = N/2$, $\mathcal{P}_{HV}(n_H, n_V, p_{HV})$ can be reexpressed using the associated Legendre polynomials as given explicitly in Eq. 3 in the main text.

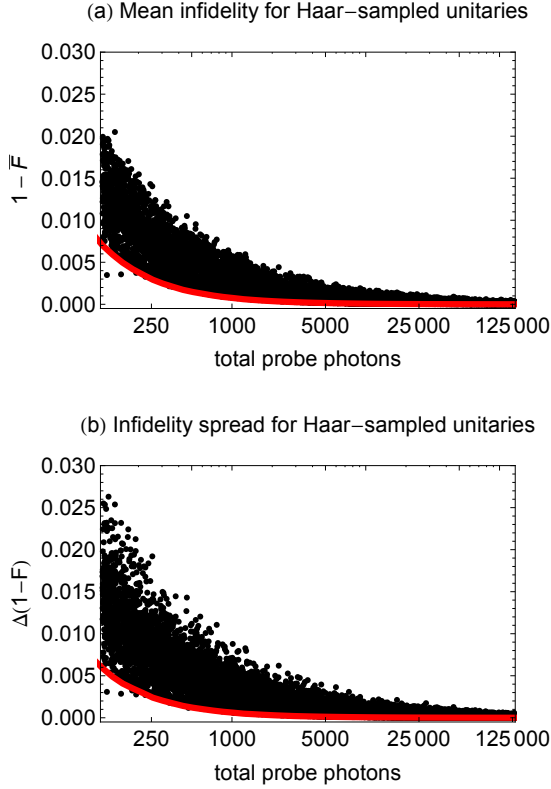


FIG. 4: These plots display the results of a simulation of our protocol for 10,000 randomly-chosen unitary operations (using the Haar-measure uniform distribution for $U(2)$). Each point corresponds to one unitary, and a randomly-chosen number of total probe photons. In every case, we assume four-photon input states: $|2, 2\rangle_{HV(DA,RL)}$. The red lines show the performance for the unitaries at the centre of the physical region: these have $a = \pm 1/2$, $b = \pm 1/2$, $c = \pm 1/2$ and $d = \pm 1/2$.

II. PERFORMANCE OF OUR PROTOCOL WITH INCREASING NUMBER OF PROBE PHOTONS

Here we present the performance of our protocol for a variety of unknown U and varying numbers of probe photons. To quantify the closeness of an estimate of \tilde{U} to U itself we use the process infidelity $1 - F$, defined as in the main text as $(1 - \min_{|\psi\rangle} |\langle \psi | \tilde{U}^\dagger U | \psi \rangle|)^2$, where the minimization is over single-photon states. The minimization can be done analytically, giving $1 - F = 1 - (a\tilde{a} + b\tilde{b} + c\tilde{c} + d\tilde{d})^2$, where $a + ib$ and $c + id$ are the transmission and reflection amplitudes for U , and $\tilde{a} + i\tilde{b}$ and $\tilde{c} + i\tilde{d}$ are the corresponding estimated values.

Fig. 4 shows the performance of our protocol for randomly-chosen U using four-photon input states. The choice of U affects both the sensitivity of each of the measurements used in the protocol, as well as the proportion of estimates (by linear inversion) that lie in the physical region; both of these factors affect the mean and spread of the infidelity (for a fixed total number of probe photons).

Fig. 5 compares the results of a simulation of the performance of our protocol with unitaries U_A and U_B for single and four-photon input states, showing how the mean and spread of the infidelity converge to 0 as the number of probe photons increases. We can observe that

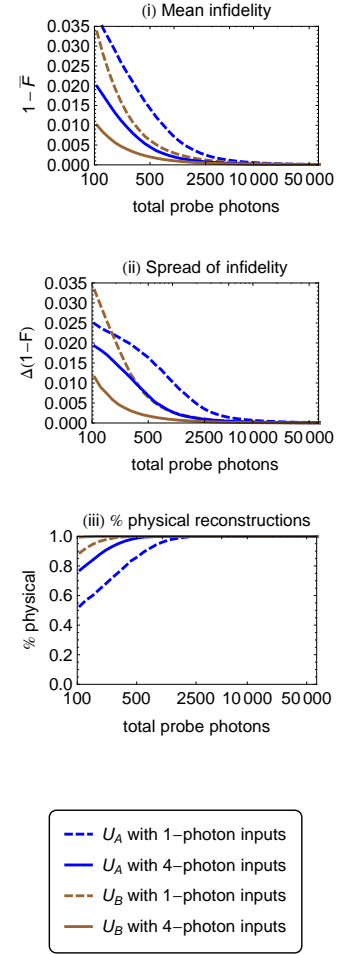


FIG. 5: The plots show the results of a simulation of the performance of our protocol for unitaries U_A and U_B , defined by comparing the cases of single-photon input states $|1, 0\rangle_{HV(DA,RL)}$ and four-photon input states, $|2, 2\rangle_{HV(DA,RL)}$.

the errors for estimating each unitary are always less using the four-photon input states in our protocol than when single-photon input states are used (for the same number of probe photons).

Acknowledgements The authors are grateful for financial support from EPSRC, ERC, NSQI, NRF (SG) and MOE (SG). JCFM is supported by a Leverhulme Trust Early-Career Fellowship. JLOB acknowledges a Royal Society Wolfson Merit Award and a RAE Chair in Emerging Technologies. We thank Tomek Paterek, Peter Turner and Sai Vinjanampathy for helpful discussions.

¹ O'Brien, J. L. *et al.* Quantum process tomography of a controlled-NOT gate. *Phys. Rev. Lett.* **93**, 080502 (2004).

² Wang, J.-Y. *et al.* Direct and full-scale experimental verifications

- towards ground-satellite quantum key distribution. *Nature Photonics* **7**, 387–393 (2013).
- ³ Yuen-Zhou, J., Krich, J. J., Mohseni, M. & Aspuru-Guzik, A. Quantum state and process tomography of energy transfer systems via ultrafast spectroscopy. *PNAS* **108**, 17615–17620 (2011).
 - ⁴ Giovannetti, V., Lloyd, S. & Maccone, L. Advances in quantum metrology. *Nature Photonics* **5**, 222–229 (2011).
 - ⁵ Riebe, M. *et al.* Process tomography of ion trap quantum gates. *Phys. Rev. Lett.* **97**, 220407 (2006).
 - ⁶ Childs, A. M., Chuang, I. L. & Leung, D. W. Realization of quantum process tomography in nmr. *Phys. Rev. A* **64**, 012314 (2001).
 - ⁷ Quantum process tomography of a universal entangling gate implemented with josephson phase qubits. *Nature Physics* **6**, 409–413 (2010).
 - ⁸ Howard, M. *et al.* Quantum process tomography and linblad estimation of a solid-state qubit. *New Journal of Physics* **8**, 33 (2006).
 - ⁹ Nambu, Y. *et al.* Experimental investigation of pulsed entangled photons and photonic quantum channels. In *Proceedings of SPIE*, vol. 4917, 13 (2002).
 - ¹⁰ De Martini, F., Mazzei, A., Ricci, M. & D’Ariano, G. M. Exploiting quantum parallelism of entanglement for a complete experimental quantum characterization of a single-qubit device. *Phys. Rev. A* **67**, 062307 (2003).
 - ¹¹ Altepeter, J. B. *et al.* Ancilla-assisted quantum process tomography. *Phys. Rev. Lett.* **90**, 193601 (2003).
 - ¹² Lobino, M. *et al.* Complete characterization of a quantum-optical processes. *Science* **322**, 563–566 (2008).
 - ¹³ Cramer, M. *et al.* Efficient quantum state tomography. *Nature Communications* **1**, 149 (2010).
 - ¹⁴ Gross, D., Liu, Y.-K., Flammia, S. T., Becker, S. & Eisert, J. Quantum state tomography via compressed sensing. *Phys. Rev. Lett.* **105**, 150401 (2010).
 - ¹⁵ Laing, A. & O’Brien, J. L. Super-stable tomography of any linear optical device. *arXiv:1208.2868*.
 - ¹⁶ Sugiyama, T., Turner, P. S. & Muraio, M. Adaptive experimental design for one-qubit state estimation with finite data based on a statistical update criterion. *Phys. Rev. A* **85**, 052107 (2012).
 - ¹⁷ Mahler, D. H. *et al.* Adaptive quantum state tomography improves accuracy quadratically. *Phys. Rev. Lett.* **111**, 183601 (2013).
 - ¹⁸ Nielsen, M. A. & Chuang, I. L. *Quantum Computation and Quantum Information* (Cambridge University Press, 2000).
 - ¹⁹ Holland, M. J. & Burnett, K. Interferometric detection of optical phase shifts at the heisenberg limit. *Phys. Rev. Lett.* **71**, 1355–1358 (1993).
 - ²⁰ Olver, F. W. *NIST handbook of mathematical functions* (Cambridge University Press, 2010).
 - ²¹ Ji, Z., Wang, G., Duan, R., Feng, Y. & Ying, M. Parameter estimation of quantum channels. *Information Theory, IEEE Transactions on* **54**, 5172–5185 (2008).
 - ²² Knysh, S. I. & Durkin, G. A. Estimation of phase and diffusion: combining quantum statistics and classical noise. *arXiv preprint arXiv:1307.0470* (2013).
 - ²³ Crowley, P. J., Datta, A., Barbieri, M. & Walmsley, I. A. Multiparameter quantum metrology. *arXiv preprint arXiv:1206.0043* (2012).
 - ²⁴ Mezzadri, F. How to generate random matrices from the classical compact groups. *Notices of the AMS* **54**, 592–604 (2007).
 - ²⁵ Thomas-Peter, N. *et al.* Real-world quantum sensors: Evaluating resources for precision measurement. *Phys. Rev. Lett.* **107**, 113603 (2011).
 - ²⁶ Reck, M., Zeilinger, A., Bernstein, H. J. & Bertani, P. Experimental realization of any discrete unitary operator. *Phys. Rev. Lett.* **73**, 58–61 (1994).
 - ²⁷ Humphreys, P. C., Barbieri, M., Datta, A. & Walmsley, I. A. Quantum enhanced multiple phase estimation. *Phys. Rev. Lett.* **111**, 070403 (2013).
 - ²⁸ Spagnolo, N. *et al.* Quantum interferometry with three-dimensional geometry. *Scientific reports* **2** (2012).
 - ²⁹ Kahn, J. Fast rate estimation of a unitary operation in $su(d)$. *Phys. Rev. A* **75**, 022326 (2007).
 - ³⁰ Ballester, M. A. Optimal estimation of $su(d)$ using exact and approximate 2-designs. *arXiv preprint quant-ph/0507073* (2005).
 - ³¹ Acin, A., Jane, E. & Vidal, G. Optimal estimation of quantum dynamics. *Phys. Rev. A* **64**, 050302 (2001).
 - ³² Hayashi, M. Parallel treatment of estimation of $su(2)$ and phase estimation. *Physics Letters A* **354**, 183–189 (2006).
 - ³³ Sperling, J., Vogel, W. & Agarwal, G. S. True photocounting statistics of multiple on-off detectors. *Phys. Rev. A* **85**, 023820 (2012).
 - ³⁴ Matthews, J. C. *et al.* Practical quantum metrology. *arXiv preprint arXiv:1307.4673* (2013).
 - ³⁵ Ritter, S. *et al.* An elementary quantum network of single atoms in optical cavities. *Nature* **484**, 195–200 (2012).
 - ³⁶ O’Brien, J. L. Optical Quantum Computing. *Science* **318**, 1567–1570 (2007).
 - ³⁷ Sakurai, J. J. Modern quantum mechanics. *Reading, MA: Addison Wesley,— c1985, edited by Tuan, San Fu* **1** (1985).
 - ³⁸ Bartlett, S. D., Rudolph, T. & Spekkens, R. W. Reference frames, superselection rules, and quantum information. *Rev. Mod. Phys.* **79**, 555–609 (2007).